

# On Coset Leader Graphs of LDPC codes

Eran Iceland and Alex Samorodnitsky \*

February 21, 2014

## Abstract

Our main technical result is that metric balls in the coset leader graph of a linear binary code of block length  $n$  spanned by constant-weight vectors grow exponentially slower than those in  $\{0, 1\}^n$ .

Following the approach of [FT05], we use this fact to improve on the first linear programming bound on the rate of LDPC codes, as the function of their minimal distance. This improvement, combined with the techniques of [BHL06], improves the rate vs distance bounds for LDPC codes in a significant sub-range of relative distances.

## 1 Introduction

This paper deals with rate versus distance bounds for binary error-correcting codes.

A binary code  $C$  of block length  $n$ , rate  $R$ , and relative minimal distance  $\delta$  is a subset of  $\{0, 1\}^n$  of cardinality  $2^{Rn}$ , such that the Hamming distance between any two distinct elements of  $C$  is at least  $d = \delta n$ . A fundamental open problem in coding theory is to find the largest possible asymptotic rate  $R = R(\delta)$  for which there exists a family of codes  $\{C_n\}_n$  with block length  $n \rightarrow \infty$ , rate at least  $R$  and distance at least  $\delta$ .

The best known bounds on  $R(\delta)$  are

$$1 - H(\delta) \leq R(\delta) \leq R_{LP}(\delta)$$

The first inequality is the Gilbert-Varshamov bound [MS77]. Here  $H(\cdot)$  is the binary entropy function. In the second inequality, we denote by  $R_{LP}(\delta)$  the *Second JPL bound* [MRRW77], obtained via the linear programming approach of Delsarte [Del73]. For an explicit expression for  $R_{LP}(\delta)$  see e.g., [Lev98].

Linear codes are an important subclass of error-correcting codes. A linear code of rate  $R$  is an  $Rn$ -dimensional linear subspace of  $\{0, 1\}^n \cong \mathbb{F}_2^n$ .

In this paper we consider a special class of linear codes. These are the LDPC (Low-Density Parity Check) codes. An LDPC code  $C$  comes with an additional parameter - an absolute

---

\*School of Engineering and Computer Science, The Hebrew University of Jerusalem, Jerusalem 91904, Israel. Research partially supported by ISF grant 1241/11 and by BSF grant 2010451.

constant  $w$ . It has an additional structure: the dual code (dual subspace)  $C^\perp$  is spanned by vectors of weight at most  $w$ .

LDPC codes were introduced by Gallager [Gal63]. They are important both in theory and in practice of robust communications. A question of interest is to investigate the rate vs. minimal distance dependence in this class of codes. Let  $R_w(\delta)$  be the largest possible asymptotic rate of an LDPC code whose dual is spanned by vectors of weight  $w$  or less.

Gallager has shown that, for large  $w$ , LDPC codes reach the Gilbert-Varshamov bound, that is

$$\limsup_{w \rightarrow \infty} R_w(\delta) \geq 1 - H(\delta)$$

From the other side, upper bounds on  $R_w(\delta)$  were obtained in [BKLM02, BHL06]. These papers use the linear programming framework, combined with direct combinatorial and information-theoretic arguments exploiting the special structure of  $C^\perp$ , to improve on the second JPL bound  $R_{LP}(\delta)$  for all values of  $\delta$ .

This paper continues the line of research started in [BKLM02, BHL06]. Our starting point is the elegant proof of the *first JPL bound*<sup>1</sup> for linear codes given in [FT05]. Given a linear code  $C$ , the strategy is to compare metric spaces defined on two graphs: the discrete cube  $\{0, 1\}^n$  and the *coset leader* graph  $\mathbb{T} = \{0, 1\}^n / C^\perp$ . Recall that we impose a multi-graph structure on  $\mathbb{T}$  by connecting  $x + C^\perp$  in  $\mathbb{T}$  to the elements of the multiset  $\{x + e_j + C^\perp\}$ ,  $j = 1, \dots, n$ .

In particular, we will be interested in how fast the metric balls  $B_{\mathbb{T}}(r) = \{x \in \mathbb{T} : d(x, 0) \leq r\}$  in  $\mathbb{T}$  grow as a function of their radius  $r$ , compared to the corresponding growth in  $\{0, 1\}^n$ . The motivation is the following (streamlined version of) result of [FT05].

**Theorem 1.1:** ([FT05]): *Let  $C$  be a linear code with relative minimal distance  $\delta$ . Let  $\mathbb{T} = \{0, 1\}^n / C^\perp$  be the coset leader graph of  $C^\perp$ . Set  $r = \left(\frac{1}{2} - \sqrt{\delta(1 - \delta)}\right) \cdot n$ . Then*

$$|C| \leq 2^{o(n)} \cdot |B_{\mathbb{T}}(r)|$$

Our main technical result is that the growth in  $\mathbb{T}$  is exponentially slower.

**Theorem 1.2:** *For any integer  $3 \leq w$  and  $0 < \rho < 1/2$ ,<sup>2</sup> there is a constant  $c = c(w, \rho) > 0$  such that the following holds for any  $n \geq w$ :*

*Let  $C \subseteq \{0, 1\}^n$  be a linear code whose dual code  $C^\perp$  is spanned by vectors of length at most  $w$ , and let  $\mathbb{T} = \{0, 1\}^n / C^\perp$ .*

*Then*

$$|B_{\mathbb{T}}(\rho n)| \leq 2^{-cn} \cdot |B(\rho n)| \tag{1}$$

Taken together with Theorem 1.1, this implies our main result, an improved upper bound on  $R_w(\delta)$ .

---

<sup>1</sup>This bound, also proved in [MRRW77], coincides with the best known bound for  $0.273... \leq \delta \leq 1/2$ .

<sup>2</sup>The case  $w = 2$  is not interesting since it is easy to see that  $R_2(\delta) = 0$  for any  $\delta > 0$ .

**Corollary 1.3:** For any  $w \geq 3$ ,

$$R_w(\delta) \leq H\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) - c\left(w, \frac{1}{2} - \sqrt{\delta(1-\delta)}\right)$$

where  $c(w, \rho)$  is given by Theorem 1.2.

**Remark 1.4:** Note that the first JPL bound for  $R(\delta)$  is

$$R(\delta) \leq H\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right)$$

Hence our bound constitutes an improvement. ■

We give explicit estimates for  $|B_{\mathbb{T}}(\rho n)|$  when  $w = 3$  and  $w = 4$ , obtaining, in particular, the following explicit bounds for  $R_3(\delta)$ :

**Theorem 1.5:** Let  $\rho = \frac{1}{2} - \sqrt{\delta(1-\delta)}$ , for  $0 \leq \delta \leq \frac{1}{2}$ . Then

$$R_3(\delta) \leq \begin{cases} \rho + \frac{1}{2}H(2\rho) & \text{if } \delta \geq \frac{1}{2} - \frac{\sqrt{2}}{3} \\ \frac{1}{3} + \frac{1}{2}H(1/3) & \text{otherwise} \end{cases}$$

**Remark 1.6:**

- Note that for  $\delta < \frac{1}{2} - \frac{\sqrt{2}}{3} \approx 0.02586$  the upper bound  $R_0 = \frac{1}{3} + \frac{1}{2}H(1/3) \approx 0.7924$  does not depend on  $\delta$ . This is simply the maximal rate an LDPC code with  $w = 3$  can have.
- The bound for  $R_3(\delta)$  looks different from the one predicted by Corollary 1.3. The reason is that we have a particular way to upper bound the metric balls in  $\mathbb{T}$  for  $w = 3$  which provides better bounds than Corollary 1.3. For a bound on  $R_4(\delta)$  which behaves according to the corollary, see Corollary A.3 in the Appendix.

■

## Comparing with known bounds

We compare the bound in Theorem 1.5 with bounds for  $R_3(\delta)$  in [BKLM02, BHL06]. Our bound is better for  $\delta$  sufficiently close to  $1/2$ . However, we can do better. The argument in [BHL06] holds if we replace the first JPL bound (which that paper uses) with our improved bound. This leads to a better bound on  $R_3(\delta)$  for  $0.156 < \delta < 1/2$ .

Note that the same line of argument leads to improved bounds for any  $w \geq 3$ . We do not attempt a detailed analysis of the interval of gain for  $w > 3$  in this paper.

**Organization.** This paper is organized as follows. We prove Theorem 1.2 in Section 2. Theorem 1.5 is proved in Section 3. Comparison with known bounds is done in Section 4. An explicit bound on  $c(4, \rho)$  is given in the Appendix.

## 2 Proof of Theorem 1.2

We start with defining the *coset leader* for a coset  $x + C^\perp \in \mathbb{T}$ . This is an element of minimal weight in the coset. If the coset has more than one element of minimal weight, we take the coset leader to be minimal in the lexicographic order among these.

In particular, a coset leader is an element of  $\{0, 1\}^n$ . Note that the metric ball  $B_{\mathbb{T}}(r)$  is the set of cosets with coset leader of Hamming weight at most  $r$ .

Our next step reduces the problem to estimating a certain probability. Given  $0 < \rho < 1/2$ , let  $x$  be a random vector in  $\{0, 1\}^n$ , obtained by setting the coordinates independently to 1 with probability  $\rho = r/n$  and to 0 with probability  $1 - \rho$ . Let  $p = p(\rho)$  be the probability that  $x$  is a coset leader. In the following discussion we may, and will, assume  $\rho n$  is an integer.

**Lemma 2.1:**

$$p(\rho) \geq \Omega\left(\frac{1}{\sqrt{n}}\right) \cdot \frac{|B_{\mathbb{T}}(\rho n)|}{|B(\rho n)|}$$

**Proof:** Note that for  $\rho < 1/2$  the function  $f(k) = \rho^k(1 - \rho)^{n-k}$  decreases in  $k$ . Recall also that (by Stirling's formula)  $|B(\rho n)| \geq \Omega\left(\frac{1}{\sqrt{n}}\right) \cdot 2^{H(\rho)n}$ . Therefore

$$p(\rho) \geq |B_{\mathbb{T}}(\rho n)| \cdot \rho^{\rho n}(1 - \rho)^{n - \rho n} = |B_{\mathbb{T}}(\rho n)| \cdot 2^{-H(\rho)n} \geq \Omega\left(\frac{1}{\sqrt{n}}\right) \cdot \frac{|B_{\mathbb{T}}(\rho n)|}{|B(\rho n)|}$$

■

Hence, we only need to argue that there exists  $c = c(w, \rho) > 0$  such that  $p < 2^{-cn}$ .

Let  $v_1, \dots, v_m$  be a basis of  $C^\perp$  whose elements are vectors of Hamming weight at most  $w$ . Identify each  $v_i$  with its support, viewed as a subset of  $\{1, \dots, n\}$ , and assume, w.l.o.g, that  $\cup_{i=1}^m v_i = \{1, \dots, n\}$ .

We partition the coordinates  $\{1, \dots, n\}$  into  $w$  disjoint sets  $I_w, I_{w-1}, \dots, I_1$ . Let  $1 \leq k \leq w$ . Suppose  $I_w, I_{w-1} \dots I_{k+1}$  are already defined, and let us define  $I_k$ . Initialize  $I_k = \emptyset$ . Go over the vectors  $v_i$ . If  $v_i$  has exactly  $k$  coordinates outside  $I_w \cup I_{w-1} \cup \dots \cup I_{k+1} \cup I_k$ , add them to  $I_k$ .

**Lemma 2.2:** Let  $A = \frac{2}{\rho^w}$  (note  $A \geq 4$ ). There exists an index  $1 \leq k \leq w$  such that

$$|I_k| > \max \left\{ A \cdot \sum_{j=k+1}^w |I_j|, \frac{n}{2wA^w} \right\}$$

**Proof:** If not, it is easy to see by induction on  $k$ , that for all  $1 \leq k \leq w$

$$|I_{w-k+1}| \leq \frac{n}{2wA^w} \cdot \sum_{j=0}^{k-1} A^j < \frac{n}{w},$$

contradicting the fact that  $|I_1| + |I_2| + \dots + |I_w| = n$ . ■

Let  $k$  be the index given by the lemma. Set  $m = |I_k|$ . Note that the coordinates of  $I_k$  are divided into  $t = m/k$  disjoint  $k$ -tuples  $u_1 \dots u_t$  and each  $u_i$  is contained in a distinct basis element  $v_{j_i}$ . Note also that  $v_{j_i} \setminus u_i$  is a subset of  $\cup_{j=k+1}^w I_j$ .

We claim that any coset leader  $x$  must contain at most  $\frac{\rho^k}{2} \cdot t$  of the  $k$ -tuples  $u_i$ . Indeed, assume not and let  $S \subset \{1 \dots t\}$  be the set of indices  $i$  such that  $u_i \subseteq x$ . Let  $y = x + \sum_{i \in S} v_{j_i}$ . Since  $x$  and  $y$  coincide on  $I_1 \cup I_2 \cup \dots \cup I_{k-1}$ , we have

$$|y| \leq |x| - k \cdot |S| + \sum_{j=k+1}^w |I_j| < |x| - \frac{\rho^k}{2} \cdot |I_k| + \sum_{j=k+1}^w |I_j| < |x|$$

where the last inequality follows from the choice of  $k$ . On the other hand,  $y$  belongs to the same coset as  $x$ , contradicting the fact that  $x$  is a coset leader.

Now, let  $x$  be a random vector with coordinates set independently to 1 with probability  $\rho = r/n$  and to 0 with probability  $1 - \rho$ . Each tuple  $u_i$  is in  $x$  with probability  $\rho^k$  and the events of containing distinct tuples are statistically independent, since the tuples are disjoint. Let  $p_0$  be the probability that  $x$  contains at most  $\frac{\rho^k}{2} \cdot t$  tuples. By the preceding discussion, and the Chernoff bound, we have, for the probability  $p$  that  $x$  is a coset leader,

$$p \leq p_0 \leq \exp \left\{ -\frac{\rho^k \cdot t}{8} \right\} \leq 2^{-cn}$$

where  $c = c(w, \rho)$  is a constant depending only on  $\rho$  and  $w$ . Taking a more detailed look at the estimates provided by Lemma 2.2, it is easy to see that  $c = c(w, \rho) \geq \frac{\log_2 e}{w^2} \cdot \left( \frac{\rho^w}{2} \right)^{w+1}$ .

### 3 Proof of Theorem 1.5

In this section, we present a sui generis argument for the case  $w = 3$ . This argument provides an explicit bound better than what we are able to derive following the line of argument in the proof of Theorem 1.2.<sup>3</sup> Unfortunately, we were not able to extend it to larger values of  $w$ .

We will argue that for any distance  $r$  attainable in  $\mathbb{T}$ , an element  $x + C^\perp$  which belongs to the  $r$ -sphere  $S_r = S_{\mathbb{T}}(r)$  around zero has at most  $n - 2r$  neighbours in the next sphere  $S_{r+1}$ . This should be compared to the behavior in the Hamming cube, in which any element in the  $r$ -sphere has  $n - r$  neighbours in the  $(r + 1)$ -sphere. A simple calculation will then show that the metric balls in the coset leader graph grow exponentially slower than in the cube, and prove the claim of the theorem.

In the following discussion we (again) identify a binary vector with its support, and assume  $\cup_{v \in C^\perp} v = \{1, \dots, n\}$ .

Consider an element  $x + C^\perp \in S_r$ , where  $x$  is the coset leader, in particular  $|x| = r$ . For each coordinate  $i \in x$  let  $v_i \in C^\perp$  be a vector of weight at most 3 containing  $i$ . The key point in the

---

<sup>3</sup>In the Appendix, we present a derivation for the case  $w = 4$ , that follows the line of argument in the proof of Theorem 1.2.

argument is that there are at least  $2r$  directions to go from  $x + C^\perp$  that *do not* lead away from zero. This is shown in the following Lemma.

**Lemma 3.1:**

1. For all  $j \in \cup_{i \in x} v_i$ ,  $d(0, x + e_j + C^\perp) \leq r$
2.  $|\cup_{i \in x} v_i| \geq 2r$  (in particular  $r \leq n/2$ )

**Proof:** First, note that  $|v_i \cap x| = 1$ , otherwise  $y = x + v_i$  would be a smaller weight element in the same coset.

Let  $j \in \cup_{i \in x} v_i$ . If  $j \in x$ , the element  $(x + e_j) + C^\perp$  is in  $S_{r-1}$ . For  $j \notin x$ , let  $j \in v_i$  for some  $i \in x$ . The vector  $x + e_j + v_i$  is of weight at most  $r$ , since  $i \in x$  and  $j \in v_i$ . Therefore  $d(0, x + e_j + C^\perp) \leq r$ .

It remains to show  $|\cup_{i \in x} v_i| \geq 2r$ .

Let  $z = \sum_{i \in x} v_i$ . Since  $v_i \cap x = \{i\}$ , clearly  $x \subseteq z$ . Note that this implies  $|z| \geq 2r$ . Otherwise, we would have  $|x + z| < r$ , and  $y = x + z$  would be a smaller weight element in the coset. Since  $z$  is supported in  $|\cup_{i \in x} v_i|$ , we have  $|\cup_{i \in x} v_i| \geq 2r$ , as required. ■

We now use this to bound the rate of growth of metric spheres in  $\mathbb{T}$ . Consider the bipartite graph whose parts are given by  $S_r$  and  $S_{r+1}$  and two vertices are connected if they are neighbours in  $\mathbb{T}$ . We have shown that the degree of any element in  $S_r$  is at most  $n - 2r$ . On the other hand, the degree of every element in  $S_{r+1}$  is, obviously, at least  $r + 1$ . By a standard double counting argument, this implies

$$|S_{r+1}| \leq \frac{n - 2r}{r + 1} \cdot |S_r|$$

Therefore, for  $r \leq n/2$  holds

$$|S_r| \leq \frac{1}{r!} \cdot \prod_{k=0}^{r-1} (n - 2k) \leq 2^r \cdot \binom{\lceil n/2 \rceil}{r}$$

and, obviously,  $S_r = 0$  for larger  $r$ .

The expression  $2^r \cdot \binom{\lceil n/2 \rceil}{r}$  increases in  $r$  till  $r = \lceil n/3 \rceil$  and decreases for larger  $r$ . Therefore (omitting the integer rounding for typographic clarity)

$$|B_{\mathbb{T}}(r)| = \sum_{k=0}^r |S_k| < \begin{cases} n \cdot 2^r \cdot \binom{n/2}{r} & \text{if } r \leq n/3; \\ n \cdot 2^{n/3} \cdot \binom{n/2}{n/3} & \text{if } r > n/3. \end{cases}$$

Substituting  $r = \rho n$  and using the inequality  $\binom{n}{\rho n} \leq 2^{nH(\rho)}$ , we obtain

$$|B_{\mathbb{T}}(\rho n)| \leq \begin{cases} 2^{n(\rho + \frac{1}{2}H(2\rho))} & \text{if } \rho \leq 1/3; \\ 2^{n(\frac{1}{3} + \frac{1}{2}H(2/3))} & \text{if } \rho > 1/3. \end{cases} \quad (2)$$

This completes the proof of Theorem 1.5. ■

## 4 Comparison to other bounds for $w = 3$

Ben Haim and Litsyn [BHL06], (see also [BKLM02]) give the best known upper bounds on the rate of LDPC codes<sup>4</sup>:

$$R(C) \leq R^{(1)}(\delta) = 1 - \frac{H(\delta/2)}{H((1 - (1 - \delta)^w)/2)} \quad (3)$$

$$R(C) \leq R^{(2)}(\delta) = 1 - \max_{\delta/2 \leq u \leq 1/2} \left( \frac{H(u) - R_{cw}(u, \delta)}{H((1 - (1 - 2u)^w)/2)} \right) \quad (4)$$

$$R(C) \leq R^{(4)}(\delta) = \min_{0 \leq t \leq 1-2\delta} \left( (1-t)R_{LP}(\delta/(1-t)) + t - \frac{t}{w} \right) \quad (5)$$

$$R(C) \leq R^{(5)}(\delta) = \min_{0 \leq t \leq 1-2\delta} \left( (1-t)R_{LP}(\delta/(1-t)) + t - \frac{t}{w-1} \right) \quad (6)$$

where  $R^{(1)}(\delta)$ ,  $R^{(2)}(\delta)$ ,  $R^{(4)}(\delta)$ , and  $R^{(5)}(\delta)$  are the bounds in Theorems 1, 2, 4 and 5 respectively of [BHL06].

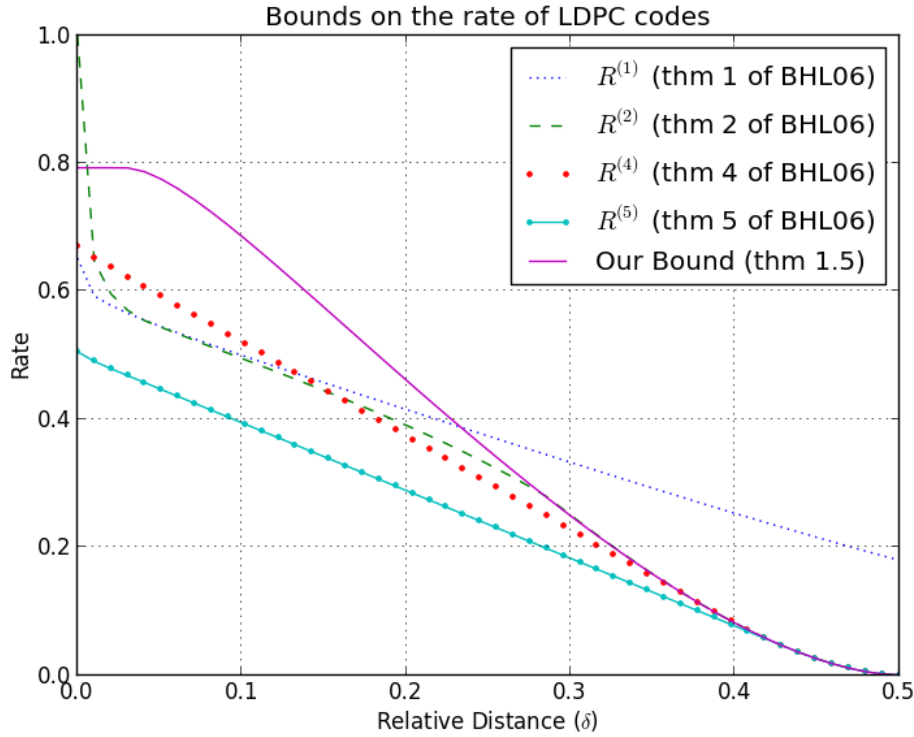


Figure 1: Bound in Theorem 1.5 and the bounds of [BHL06]

The combined plots above require an explanation. First,  $R^{(5)}$  is the best of [BHL06] bounds for the whole range  $0 < \delta < 0.5$ . However, it requires an additional assumption, namely that the

<sup>4</sup> $R_{LP}$  is the second JPL bound. For the definition of  $R_{cw}$  see [BHL06].

weight of each column in the parity check matrix is at least 2. Without this assumption, we are left with the bounds  $R^{(1)}$ ,  $R^{(2)}$  and  $R^{(4)}$ , each of which is optimal in a subrange of  $0 < \delta < 0.5$ .

Our bound is better than  $R^{(4)}$  for  $\delta > 0.3877$  and better than  $R^{(5)}$  for  $\delta > 0.4387$ , since for these values of  $\delta$  the two bounds, are very close to the first linear programming bound.

However, we can do better. The argument in Theorems 4 and 5 in [BHL06] holds if we replace  $R_{LP}$  with the better bound of Theorem 1.5 (since the first and the second JPL bounds coincide in this case). This leads to a (small) improvement on  $R^{(4)}$  and  $R^{(5)}$ , and hence to best known bounds when these two bounds are optimal. ( $R^{(4)}$  is optimal for  $0.156 < \delta < 1/2$ ).

To sum up, we improve the bounds on  $R_3(\delta)$  for  $0.156 < \delta < 1/2$ . Given the additional assumption that the weight of each column in the parity check matrix is at least 2, we improve the bounds on the rate for the whole range  $0 < \delta < 0.5$ .

## References

- [BHL06] Yael Ben-Haim and Simon Litsyn. Upper bounds on the rate of LDPC codes as a function of minimum distance. *IEEE Trans. Inform. Theory*, 52(5):2092–2100, 2006.
- [BKLM02] David Burshtein, Michael Krivelevich, Simon Litsyn, and Gadi Miller. Upper bounds on the rate of LDPC codes. *IEEE Trans. Inform. Theory*, 48(9):2437–2449, 2002.
- [Del73] Philippe Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.
- [FT05] Joel Friedman and Jean-Pierre Tillich. Generalized Alon-Boppana theorems and error-correcting codes. *SIAM J. Discrete Math.*, 19(3):700–718 (electronic), 2005.
- [Gal63] Robert Gallager. Low-density parity-check codes. *MIT press*, 1963.
- [Lev98] Vladimir I. Levenshtein. Universal bounds for codes and designs. In *Handbook of coding theory, Vol. I, II*, pages 499–648. North-Holland, Amsterdam, 1998.
- [MRRW77] Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey, Jr., and Lloyd R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Information Theory*, IT-23(2):157–166, 1977.
- [MS77] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.



## A Bounds on $|B_{\mathbb{T}}(r)|$ for $w = 4$

The main result of this section is an explicit lower bound on  $c(4, \rho)$ , the constant in Theorem 1.2. We show

$$c(4, \rho) \geq \frac{\rho}{2} \cdot \log_2 \left( \frac{1}{(1-\rho)^4 + 4\rho(1-\rho)^3 + 6\rho^2(1-\rho)^2} \right) - o_n(1) \quad (7)$$

This implies the corresponding upper bound on  $R_4(\delta)$  via Corollary 1.3.

**Corollary A.1:** *Let  $\rho = \sqrt{\frac{1}{2} - \delta(1-\delta)}$ . Then*

$$R_4(\delta) \leq H(\rho) - \frac{\rho}{2} \cdot \log_2 \left( \frac{1}{(1-\rho)^4 + 4\rho(1-\rho)^3 + 6\rho^2(1-\rho)^2} \right)$$

Let  $I_1, I_2, I_3, I_4$  be the partition of  $[n]$  defined in the proof of Theorem 1.2. Denote:

$$|I_1| = \alpha_1 n, \quad |I_2| = \alpha_2 n, \quad |I_3| = \alpha_3 n, \quad |I_4| = \alpha_4 n$$

Note that  $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$ .

We start with a lemma that shows that we can find elements of a prescribed structure in each coset of  $C^\perp$ . Both in the statement and in the proof of the lemma we refer to the properties of  $I_j$  as described in the proof of Theorem 1.2.

**Lemma A.2:** *Let  $u \in \{0, 1\}^n$ .*

1. *There is an element  $u_1 \in u + C^\perp$  that does not intersect  $I_1$ .*
2. *There is an element  $u_2 \in u + C^\perp$  whose weight is at most that of  $u$  and such that*
  - $u_2 \cap I_1 = u \cap I_1$ .
  - $u_2$  intersects each pair of  $I_2$  in at most one coordinate.
  - $u_2$  intersects each triple of  $I_3$  in at most one coordinate.
  - $u_2$  intersects each 4-tuple of  $I_4$  in at most two coordinates.

Before proving the lemma, we state two corollaries.

**Corollary A.3:**

1. *Each coset of  $C^\perp$  has a representative that does not intersect  $I_1$  at all; intersects each pair of  $I_2$  in at most one coordinate; intersects each triple of  $I_3$  in at most one coordinate; and intersects each 4-tuple of  $I_4$  in at most two coordinates.*
2. *Each coset of  $C^\perp$  has a minimal weight representative that intersects each pair of  $I_2$  in at most one coordinate; intersects each triple of  $I_3$  in at most one coordinate; and intersects each 4-tuple of  $I_4$  in at most two coordinates.*

**Proof:**

1. Apply both parts of the lemma to any element  $u$  in the coset.
2. Apply the second part of the lemma to a minimal weight element  $u$  in the coset.

■

**Corollary A.4:** *The diameter of the coset leader graph  $\mathbb{T} = \{0,1\}^n/C^\perp$  is at most  $D = (\alpha_2/2 + \alpha_3/3 + \alpha_4/2) \cdot n$ .*

**Proof:**

Since  $\mathbb{T}$  is vertex-transitive, it suffices to show that the distance of any coset of  $C^\perp$  from zero is at most  $D$ . That is, each coset of  $C^\perp$  contains an element of weight at most  $D$ .

Indeed, any coset has a representative with a structure given by the first part of Corollary A.3. It is immediate that its weight is at most  $D$ . ■

### Proof of Lemma A.2

The first part of the lemma. For each coordinate  $i \in I_1$  contained in  $u$ , add to  $u$  a basis vector  $v_i \in C^\perp$  that intersects  $I_1$  only in this coordinate. This process results in an element  $u_1$  in the same coset, whose intersection with  $I_1$  is empty.

The second part of the lemma. We modify  $u$  in three steps, by adding vectors from  $C^\perp$ , until we arrive to the desired structure. We observe that the weight of  $u$  does not increase in the process.

1. For each pair  $(i, j)$  in  $I_2$  contained in  $u$ , add to  $u$  a basis vector  $v \in C^\perp$  of weight at most four containing the pair, whose remaining 1-coordinates are in  $I_3 \cup I_4$ . Note that this does not increase the weight of  $u$  and does not affect its intersection with  $I_1$ . At the end of this step we arrive to an element  $u' \in u + C^\perp$  intersecting each pair of  $I_2$  in at most one coordinate.
2. For each triple in  $I_3$  that intersects  $u'$  in at least two coordinates, add to  $u'$  a basis vector  $v \in C^\perp$  of weight at most four that contains the triple, and whose remaining 1-coordinate (if it exists) is in  $I_4$ . Note that this, again, does not increase the weight of  $u'$  and does not affect its intersection with  $I_1$  and  $I_2$ . This step terminates at an element  $u''$  of the same coset whose intersections with  $I_1$ ,  $I_2$  and  $I_3$  are as required.
3. For each 4-tuple in  $I_4$  that intersects  $u''$  in more than two coordinates, add it to  $u''$ . As above, this does not increase the weight of  $u''$  and does not affect its intersection with  $I_1$ ,  $I_2$ ,  $I_3$ . At the end of the process we obtain an element  $u_2 \in u + C^\perp$  whose intersections with  $I_j$ ,  $j = 1, \dots, 4$  are as required.

■

We proceed to upper bound the cardinalities  $|B_{\mathbb{T}}(r)|$  of metric balls in  $\mathbb{T}$ . By Corollary A.4, it suffices to analyze  $|B_{\mathbb{T}}(r)|$  for  $r \leq (\frac{\alpha_2}{2} + \frac{\alpha_3}{3} + \frac{\alpha_4}{2}) \cdot n$ . Let us fix such  $r$  and set  $\rho = r/n$ .

Consider the following probabilistic experiment. Let  $x \in \{0, 1\}^n$  be a random vector whose coordinates are independently set to 1 with probability  $\rho$  and to 0 with probability  $1 - \rho$ . Let  $p = p(\rho)$  be the probability that  $x$  is of minimal weight in its coset and has the structure described in the second part of Corollary A.3. Note that each coset has exactly one coset leader and at least one element with the properties described in the corollary. Therefore  $p$  is greater or equal than the probability of  $x$  to be a coset leader. Hence, by Lemma 2.1, it is enough to upper bound  $p$ .

The constraints on  $x$  arising from its constrained intersections with elements of  $I_j$ ,  $j > 1$ , are independent. The probability for all of them to hold is

$$((1 - \rho)^4 + 4\rho(1 - \rho)^3 + 6\rho^2(1 - \rho)^2)^{\frac{1}{4}\alpha_4 n} \cdot ((1 - \rho)^3 + 3\rho(1 - \rho)^2)^{\frac{1}{3}\alpha_3 n} \cdot (1 - \rho^2)^{\frac{1}{2}\alpha_2 n} \quad (8)$$

We want to maximize this expression over the domain

$$\Delta(\rho) = \left\{ \alpha_1, \alpha_2, \alpha_3, \alpha_4 \geq 0, \quad \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1, \quad \alpha_2/2 + \alpha_3/3 + \alpha_4/2 \geq \rho \right\}$$

We argue that for fixed  $\alpha_1$ , this expression is maximized when  $\alpha_2 = \alpha_3 = 0$  and  $\alpha_4 = 1 - \alpha_1$ . We start with a technical lemma:

**Lemma A.5:** *For any  $0 \leq \rho \leq 1/2$ ,*

$$((1 - \rho)^4 + 4\rho(1 - \rho)^3 + 6\rho^2(1 - \rho)^2)^{\frac{1}{4}} \geq \max \left\{ ((1 - \rho)^3 + 3\rho(1 - \rho)^2)^{\frac{1}{3}}, (1 - \rho^2)^{\frac{1}{2}} \right\}$$

**Proof:** Dividing out by  $(1 - \rho)^{1/2}$  and rearranging, it suffices to show:

$$((1 + \rho)^2 + 2\rho^2)^{1/4} \geq (1 + \rho)^{1/2} \geq (1 - \rho)^{1/6}(1 + 2\rho)^{1/3}$$

The first inequality follows by comparing the fourth power of the two terms.

For the second inequality, observe that

$$(1 + \rho)^3 - (1 - \rho)(1 + 2\rho)^2 = \rho^2 - \rho^3 \geq 0$$

■

By the lemma, increasing  $\alpha_4$  and decreasing  $\alpha_2 + \alpha_3$  by the same amount increases (8) and leaves us in  $\Delta(\rho)$  as long as  $\alpha_2, \alpha_3 \geq 0$ .

Hence, we may take  $\alpha_2 = \alpha_3 = 0$  and  $\alpha_4 = 1 - \alpha_1$ .

We arrive to the problem of maximizing  $((1 - \rho)^4 + 4\rho(1 - \rho)^3 + 6\rho^2(1 - \rho)^2)^{\frac{1}{4}\alpha_4 n}$  on  $[2\rho, 1]$ .

Since  $((1 - \rho)^4 + 4\rho(1 - \rho)^3 + 6\rho^2(1 - \rho)^2) < 1$ , the maximum is attained at  $\alpha_4 = 2\rho$ . Hence

$$p \leq ((1 - \rho)^4 + 4\rho(1 - \rho)^3 + 6\rho^2(1 - \rho)^2)^{\frac{1}{2}\rho n},$$

concluding the proof of (7).